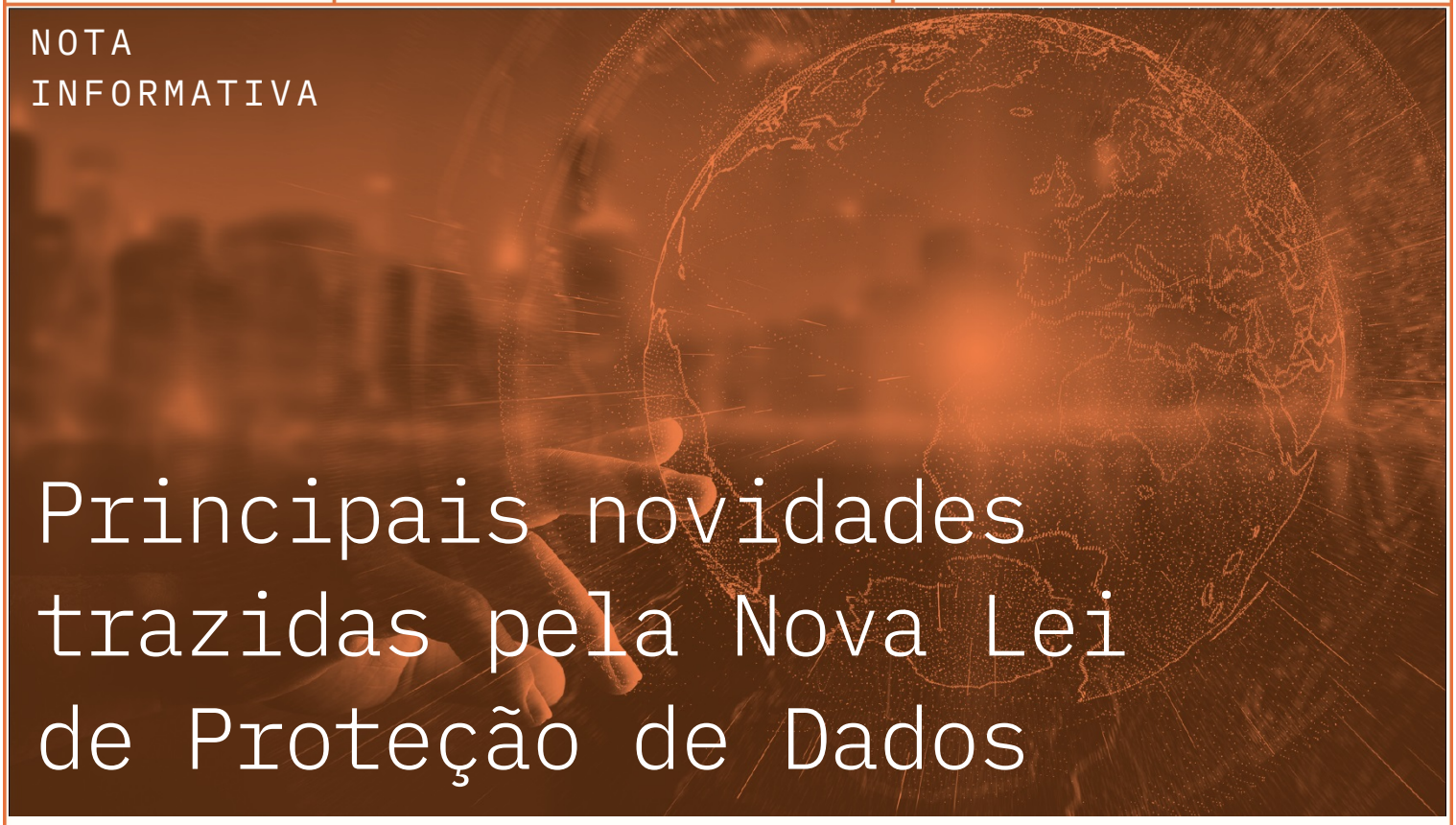
NOTA INFORMATIVA



Principais novidades trazidas pela Nova Lei de Proteção de Dados

1. Aplicação territorial

Relativamente à aplicação territorial, a lei de execução na ordem jurídica interna do RGPD determina que as regras relativas ao tratamento de dados pessoais previstas na Lei n.º 58/2019 e no RGPD, são aplicáveis aos dados pessoais inscritos nos postos consulares pertencentes a portugueses residentes no estrangeiro.

2. Atribuições e competências da Comissão Nacional de Proteção de Dados

Para além das atribuições e competências que o artigo 57.º do RGPD atribui às autoridades de controlo (no nosso caso a Comissão Nacional de Proteção de Dados – CNPD), a lei de execução na ordem jurídica interna do RGPD atribui às referidas entidades as seguintes competências:

- Pronunciar-se, a título não vinculativo, sobre as medidas legislativas e regulamentares relativas à proteção de dados pessoais, bem como sobre instrumentos jurídicos em preparação, em instituições europeias ou internacionais, relativos à mesma matéria;

- Fiscalizar o cumprimento das disposições do RGPD e das demais disposições legais e regulamentares relativas à proteção de dados pessoais e dos direitos, liberdades e garantias dos titulares dos dados, e corrigir e sancionar o seu incumprimento;

- Disponibilizar uma lista de tratamentos sujeitos à avaliação do impacto sobre a proteção de dados, nos termos do n.º 4 do

artigo 35.º do RGPD, definindo igualmente critérios que permitam densificar a noção do conceito de "elevado risco";

- Elaborar e apresentar ao Comité Europeu para a Proteção de Dados, os projetos de critérios para a acreditação dos organismos de monitorização de códigos de conduta e dos organismos de certificação;

- Cooperar com o Instituto Português de Acreditação, I.P. (IPAC, I.P.), relativamente à acreditação e certificação dos organismos a título de proteção de dados, bem como na definição de requisitos adicionais de acreditação, nesta área.

3. Dever de colaboração com a CNPD

As entidades públicas e privadas devem colaborar com a CNPD, facultando-lhes todas as informações que lhes sejam solicitadas. O dever de colaboração é assegurado, designadamente, quando a CNPD tiver necessidade, para o cabal exercício das suas funções, de examinar o sistema informático e os ficheiros de dados pessoais, bem como toda a documentação relativa ao tratamento e transmissão de dados pessoais.

A falta de colaboração com a CNPD constitui uma contraordenação grave punida com coima:

- De €2.500,00 a €10.000.000,00 ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de uma empresa grande;

- De €1.000,00 a 1.000,000,00 ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de PME;

- De €500,00 a €250.000,00, no caso de pessoas singulares.

4. Encarregado de proteção de dados

O Encarregado de Proteção de dados não carece de certificação profissional.

Para além das funções que lhe são confiadas nos termos dos artigos 37.º a 39.º do RGPD, terá ainda, nos termos da Lei n.º 58/2019, cabem-lhe ainda as seguintes funções:

- Assegurar a realização de auditorias, quer periódicas, quer não programadas de proteção de dados;

- Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;

- Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados.

5. Acreditação, certificação e códigos de conduta

// Os selos e marcas de proteção de dados servem para atestar que os procedimentos implementados cumprem o disposto no RGPD e na presente Portuguesa de execução interna daquele Regulamento;

// A autoridade competente em Portugal para realizar a acreditação dos organismos de certificação em matéria de proteção de dados é o IPAC, I.P.

// A certificação, bem como a emissão de selos e marcas de proteção de dados, é efetuada por organismos de certificação acreditados junto do IPAC, I.P.

6. Consentimento de menores para tratamento dos seus dados pessoais

// Os dados pessoais de crianças só podem ser objeto de tratamento com base no seu consentimento, relativamente à oferta direta de serviços da sociedade de informação, quando as mesmas tenham completado treze anos de idade;

// No caso de menores com idade inferior a treze anos, o tratamento dos seus dados só é lícito se tiver sido dado pelos seus representantes legais, de preferência com recurso a meios de autenticação segura.

7. Proteção de dados pessoais de pessoas falecidas

Os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD e da Lei n.º 58/2019 sempre que:

- Digam respeito a informação que revele a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, ou dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa;
- Quando se reportem à intimidade da vida privada;
- Digam respeito à imagem ou aos dados relativos às comunicações, **ressalvados** os casos em que:
  - Tenha havido o consentimento explícito do titular dos dados;
  - O tratamento for necessário para efeitos de obrigações e do exercício de direitos específicos do responsável pelo tratamento de dados em matéria de legislação laboral, de segurança social e de proteção social;
  - O tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar fisicamente ou legalmente incapacitado de dar o seu consentimento;
  - Se o tratamento for efetuado, no âmbito das suas atividades legítimas de uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, desde que esse tratamento diga respeito aos membros ou antigo membros, os dados não sejam comunicados a terceiras entidades e tenham sido implementadas garantias

adequadas;

- Estejam em causa dados que tenham sido manifestamente tornados públicos pelo seu titular;
- Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial;
- Se o tratamento for necessário por motivos de interesse público importante;
- Se o tratamento de dados for necessário para efeitos de medicina preventiva ou do trabalho, avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social;
- Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública;
- Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos.

➢ Os direitos previstos relativamente aos dados pessoais de pessoas falecidas, são exercidos por quem a pessoa falecida haja designado para o efeito, ou na sua falta, pelos respetivos herdeiros;

➢ Os titulares dos dados podem deixar determinada a impossibilidade de exercício dos direitos relativos aos seus dados pessoais.

8. Videovigilância

Os sistemas de videovigilância, para além de terem de estar em sintonia com o artigo 31-º da Lei 34/20133, de 16 de maio (que estabelece o regime do exercício da atividade de segurança privada), não podem incidir sobre:

➢ Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;

➢ Zonas de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM;

➢ O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;

➢ Zonas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.

Nos casos em que é autorizada a videovigilância, **é proibida a captação de som, exceto:**

➢ Se for requerida uma autorização prévia à CNPD;

- No período em que as instalações vigiadas estão encerradas.

9. Prazo de conservação de dados pessoais

Relativamente à conservação dos dados a lei estabelece que:

- O prazo de conservação dos dados deve ser o que estiver fixado por lei e na falta deste, o prazo que se revele necessário para a prossecução da finalidade;
- Quando os dados sejam necessários para fazer prova do cumprimento de obrigações contratuais ou de outra natureza, os dados podem ser conservados enquanto não decorrer o prazo de prescrição;
- Os dados relativos a declarações contributivas para efeitos de aposentação ou reforma podem ser conservados sem limite de prazo, a fim de auxiliar o titular na reconstituição das carreiras contributivas.

10. Tratamento de dados pessoais por entidades públicas para finalidades diferentes

A lei passa a permitir que entidades públicas, que tenham recolhido dados pessoais para uma especifica e determinada finalidade:

- Utilizem esses mesmos dados para outras finalidades, e
- Transmitam esses dados e outras entidades públicas, para cumprimento de finalidades de tratamento diferentes daquelas que justificaram a sua recolha inicial, desde que:
  - tenha natureza excecional;
  - vise assegurar a prossecução do interesse público que de outra forma não possa ser acautelado;
  - seja devidamente fundamentado.

11. Liberdade de expressão e informação

A proteção de dados pessoais, nos termos do RGPD não prejudica o exercício da liberdade de expressão, informação e imprensa, incluindo o tratamento de dados para fins jornalísticos e para fins de expressão académica, artística ou literária.

O exercício da liberdade de informação, especialmente quando revele dados de categorias especiais[1], deve respeitar o princípio da dignidade da pessoa humana, bem como os direitos de personalidade.

O exercício da liberdade de expressão não legitima a divulgação de dados pessoais como moradas e contactos, à exceção daqueles que sem de conhecimento generalizado.

12. Publicação em jornal oficial

A publicação de dados pessoais em jornais oficiais deve respeitar os princípios da finalidade e da minimização de dados. Como tal, sempre que o dado pessoal nome, seja

[1] Dados de categorias especiais: aqueles que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

suficiente para garantir a identificação do titular e a eficácia do tratamento, não devem ser publicados outros dados pessoais.
O direito ao apagamento quanto a dados pessoais publicados em jornal oficial tem natureza excecional, e só deverá ocorrer quando for a única forma de acautelar o direito ao esquecimento e ponderados os demais interesses em presença.

O exercício do direito ao apagamento relativamente a publicações em jornal oficial na internet será feito por via da desindexação (para que o resultado deixe de aparecer como resultado de pesquisa no motor de busca) mas nunca deve ser eliminada a própria publicação/fonte.

13. Relações laborais

// Salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais:

- se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador; ou
- se esse tratamento for necessário para a execução de um contrato no qual o trabalhador é parte ou a seu pedido para diligência pré-contratuais.

// As imagens gravadas e outros dados pessoais registados através de sistemas de videovigilância ou outros meios tecnológicos, só podem ser utilizados no âmbito do processo penal e para apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal.

// O tratamento de dados biométricos dos trabalhadores só é considerado legítimo para:

- controlo de assiduidade; e
- controlo de acessos às instalações do empregador.

// Apenas podem ser utilizadas representações dos dados biométricos e deverá ser garantido que o respetivo processo de recolha não permite a reversibilidade dos dados.

14. Tratamento de dados de saúde e dados genéticos

Nos tratamentos de dados de saúde e de dados genéticos o acesso aos dados rege-se pelo princípio da necessidade de conhecer a informação.

O tratamento de dados de categorias especiais para efeito de medicina preventiva ou do trabalho, avaliação da capacidade de trabalho do empregado, diagnóstico médico, prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social deverá ser efetuado por um profissional obrigado a sigilo, ou por pessoa sujeita a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação.

A lei prevê ainda um dever de sigilo a todos os profissionais que, no contexto do acompanhamento, financiamento ou fiscalização da atividade de prestação de cuidados de saúde, tenham acesso a dados relativos à saúde.

É ainda imposta a obrigação de notificação do titular dos dados de qualquer acesso realizado aos seus

dados pessoais, cabendo ao responsável pelo tratamento assegurar a disponibilização desse mecanismo de rastreabilidade e notificação.

As medidas mínimas de segurança inerentes aos tratamentos de dados de saúde e dados genético, será aprovado por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça.

15. Contraordenações

Para além das situações que o RGPD considera integram uma contraordenação, a lei de execução na ordem jurídica interna daquele Regulamento, prevê ainda como **contraordenações graves**:

- A falta de colaboração com a CNPD;
- A não prestação da informação ao titular dos dados;
- Violação das normas relativas às obrigações impostas pelo RGPD ao Responsável pelo tratamento dos dados e a inobservância do Princípio da Proteção de dados desde a conceção e por defeito;
- A violação das obrigações por parte dos responsáveis conjuntos pelo tratamento de dados;
- A violação das obrigações relativas à designação de um representante, por parte de responsáveis pelo tratamento de dados ou subcontratantes, não estabelecidos na União Europeia;
- A violação das obrigações relativas aos subcontratantes;
- O tratamento de dados pessoais por parte de subcontratantes (ou subcontratantes destes), sem as necessárias instruções do responsável pelo tratamento;
- A ausência dos registos dos tratamentos de dados pessoais, exigidos pelo artigo 30º do RGPD;
- A violação das regras de segurança previstas no artigo 32º do RGPD;
- A falta de notificação de uma violação de dados pessoais à CNPD ou ao titular dos dados;
- A violação de realização de avaliações de impacto;
- A omissão de consulta prévia da CNPD nos casos e que tal consulta é obrigatória;
- A falta de designação de encarregado de proteção de dados quando a lei o imponha;
- A violação das normas relativas à posição do encarregado de proteção de dados, em especial, no que respeita às garantias de independência que este deve ter dentro da organização;
- O incumprimento das funções atribuídas ao encarregado da proteção de dados;
- A prática de atos de supervisão de códigos de conduta por organismos não acreditados pela autoridade de controlo;
- Violação por parte dos organismos de supervisão de códigos de conduta da obrigação de informar a CNPD das violações conhecidas ao código adotado;
- A utilização de selos e marcas de proteção de dados que não tenham sido emitidos por entidades

certificadoras;

- O incumprimento por parte dos organismos de certificação das obrigações que para estas entidades resultam do artigo 43º do RGPD;
- Violação das regras previstas na lei relativas à videovigilância.

Os comportamentos acima descritos, serão punidos com coima:

a) De €2.500,00 a €10 000 000,00 ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de grande empresa;

b) De €1.000,00 a €1 000 000,00 ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de PME;

c) De €500,00 a €250.000,00 tratando-se de pessoa singular.

Para além das contraordenações descritas no RGPD a lei de execução na ordem jurídica interna daquele Regulamento, prevê ainda como **contraordenações muito graves**:

- O tratamento de dados pessoas com a inobservância dolosa dos princípios consagrados no artigo 5.º do RGPD;
- O tratamento de dados pessoais sem condição adequada de legitimidade;
- A violação das regras relativas à prestação do consentimento;
- O tratamento de categorias especiais de dados fora dos casos permitidos por lei;
- O tratamento de dados pessoais relacionados com condenações penais e infrações, fora dos casos legalmente admissíveis;
- A exigência de pagamento de uma quantia em dinheiro para prestação de informações aos titulares dos dados, fora dos casos previstos no RGPD;
- A exigência de pagamento de uma quantia em dinheiro, em que a lei o permite, mas que exceda os custos necessários para a satisfazer o direito do titular dos dados;
- A falta de prestação de informações relevantes ao titular dos dados, nomeadamente:
  - omissão de informação das finalidades a que se destina o tratamento;- omissão de informação acera dos destinatários ou categorias de destinatários dos dados pessoais;
  - omissão de informação acerca do direito de retirar o consentimento, nos casos em que o tratamento tenha por base o consentimento.
- Não permitir, não assegurar ou dificultar o exercício dos direitos dos titulares dos dados;
- A transferência internacional de dados em violação do RGPD;
- O incumprimento das decisões da autoridade de controlo ou recusa em colaboração que lhe seja exigida pela CNPD.

Os comportamentos acima descritos, serão punidos com coima:

d) De €5.000,00 a €20 000 000,00 ou 4% do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de grande empresa;

e) De €2.000,00 a €2 000 000,00 ou 4% do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de PME;

f) De €1.000,00 a €500 000,00 tratando-se de pessoa singular.

16. Crimes

A Lei n.º 58/2019 prevê os seguintes crimes:

- Utilização de dados de forma incompatível com a finalidade da recolha;
- Acesso indevido;
- Desvio de dados;
- Viciação ou destruição de dados;
- Inserção de dados falsos;
- Violação do dever de sigilo;
- Desobediência.

Para mais informações contactar:

DEPARTAMENTO DE TECNOLOGIAS, MEDIA & TELECOMUNICAÇÕES

Martim Bouza Serrano – mbs@cca.law

www.cca.law